dishNET Wireline L.L.C.
9601 S. Meridian Blvd.
Englewood, CO 80112

March 1, 2019

**VIA ELECTRONIC FILING**

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th St., SW
Washington, DC 20554

RE: Annual CPNI Certification, EB Docket No. 06-36

Dear Ms. Dortch:

Pursuant to Section 64.2009(e) of the Commission's rules, 47 C.F.R. 64.2009(e), dishNET Wireline L.L.C. files its annual certification of compliance with the Commission's customer proprietary network information (CPNI) rules.

Sincerely,

/s/
**Jeffrey H. Blum**
*Senior Vice President, Public Policy and Government Affairs*

**Annual 47 C.F.R. § 64.2009(e) CPNI Certification**

**EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2019 covering the prior calendar year 2018

1. Date filed: March 1, 2019

2. Name of company covered by this certification: dishNET Wireline, L.L.C ("Company")

3. Form 499 Filer ID: 824050

4. Name of signatory: Jeffrey H. Blum

5. Title of signatory: Senior Vice President, Public Policy and Government Affairs

6. Certification:

I, Jeffrey H. Blum, certify that I am an officer of the Company named above, and acting as an agent of the Company, that based upon personal knowledge or on information provided to me, the Company has operating procedures that are adequate to comply with the Federal Communications Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the Company's procedures comply with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

I certify under penalty of perjury that the foregoing certification is true and correct to the best of my current knowledge, information, and belief.

Signed: _____

Date: 3/1/

Attachment: Statement Concerning the Protection of Customer Proprietary Network Information

# Statement Concerning the Protection of Customer Proprietary Network Information

1. dishNET Wireline L.L.C. is a telecommunications carrier subject to the requirements set forth in Section 64.2001 *et seq.* of the Federal Communications Commission's ("FCC's") rules. The Company has established operating procedures applicable to the FCC's rules pertaining to the use, disclosure and access to customer proprietary network information ("CPNI").

2. Training provides Company personnel, agents, and contractors (as applicable) with information as to when they are and are not authorized to release or use CPNI. Violation of these policies will subject personnel to appropriate disciplinary/remedial action.

3. If a customer calls the Company requesting information that is considered CPNI, the Company will not release such information unless the customer is able to verify he or she is the authorized party on the account through provision of a password. If the customer cannot supply the password, the customer may be asked a series of challenge and answer questions, or may request that the information be sent to the customer's address of record.

4. If a customer requests online access to information that is considered CPNI, the Company will not allow online access to such information unless the customer is able to verify he or she is the authorized party on the account through provision of a password. If the customer cannot supply the password, the customer is directed to contact customer service.

5. The Company will not use, disclose, or permit access to CPNI to identify or track customers that call competing service providers.

6. If and when customer approval to use, disclose, or permit access to customer CPNI is desired, the Company will obtain such customer approval. The Company honors a customer's approval or disapproval until the customer revokes or limits such approval or disapproval.

7. The Company does not use CPNI information for sales and marketing campaigns.

8. Prior to any solicitation for customer approval to use CPNI for sales and marketing campaigns, the Company will provide notification to customers of their right to restrict use of, disclosure of, and access to the customer's CPNI. Records of these notifications will be maintained for a period of at least one year.

9. Any customer request to deny access to CPNI will not affect the provision of any services to which the customer subscribes.

10. If a breach of CPNI occurs, the Company will provide electronic notification of the breach to the U.S. Secret Service ("USSS") and the FBI as soon as practicable and in no event more than seven (7) days after reasonable determination of the breach. The Company will also notify impacted customer(s) only after seven (7) more days have passed after notification to the USSS and the FBI, unless there is a risk of immediate and irreparable harm to the customer in which case the Company will notify the customer immediately after consulting with and in cooperation with the relevant investigative agency. Company will keep records or discovered breaches for at least two (2) years.